

Amendments to the Claims

Please replace all previous versions of the claims with the following listing:

1. (Cancelled)
2. (Currently Amended) The method of claim ~~[[1]]~~ 16, wherein the encryption method is called a Block Cipher SQUARE encryption method.
3. (Currently Amended) The method of claim ~~[[1]]~~ 16, further comprising the step of decrypting the engraved signature before comparing with the computed signature where the engraved signature has been encrypted.
4. (Previously Presented) The method of claim 3, wherein the step of decrypting the engraved signature includes using another encryption method.
5. (Currently Amended) The method of claim ~~[[1]]~~ 16, wherein the identifier comprises at least one of a MAC address of a Network Interface Card, a serial number of a CPU, a hard drive format code number, and a code number of computer system "add-ons".
6. (Cancelled)
7. (Currently Amended) The system of claim ~~[[6]]~~ 17, wherein the encryption method is called a Block Cipher SQUARE encryption method.
8. (Currently Amended) The system of claim ~~6, further comprising 17, wherein~~ the authentication program ~~decrypting~~ decrypts the engraved signature before

comparing the engraved signature with the computed signature where the engraved signature has been encrypted.

9. (Previously Presented) The system of claim 8, wherein the engraved signature has been encrypted and decrypted using another encryption method.

10. (Currently Amended) The system of claim [[6]] 17, wherein the identifier comprises at least one of a MAC address of a Network Interface Card, a serial number of a CPU, a hard drive format code number, and a code number of computer system "add-ons".

11. (Currently Amended) An article comprising:

a computer-readable signal-bearing medium including a software application;

the medium including an associated engraved signature, the engraved signature being initially blank such that the software application can be ~~authenticated for use~~ initially be used on one of a plurality of computer systems but once used on a computer system is authenticated for that particular computer system;

the medium further including an authentication program for authenticating the software application for use on the computer system;

during execution of the software application, the authentication program for reading the engraved signature and,

if the engraved signature is not blank then the authentication program performing the following:

retrieving the identifier from the computer system;

encrypting the identifier using an encryption method to obtain a computed signature;

comparing the computed signature to the engraved signature; and
~~halting-inhibiting~~ execution of the software application if the
computed signature does not match the engraved signature; and

if the engraved signature is blank, then performing the following:

retrieving the identifier from the computer system;

encrypting the identifier using the encryption method to obtain a
computed signature; and

storing the computed signature as the engraved signature thereby
generating the engraved signature at the computer system on which the software
application is being executed and authenticating the software application only for
that computer system.

12. (Currently Amended) The article of claim 11, wherein the encryption method
is called a Block Cipher SQUARE encryption method.

13. (Currently Amended) The article of claim 11, further ~~comprising-wherein~~ the
authentication program ~~decrypting-decrypts~~ the engraved signature before
comparing with the computed signature where the engraved signature has been
encrypted.

14. (Cancelled)

15. (Original) The article of claim 11, wherein the identifier comprises at least one
of a MAC address of a Network Interface Card, a serial number of a CPU, a hard
drive format code number, and a code number of computer system "add-ons".

16. (New) A method of authenticating a software application loaded on a
computer system having an identifier associated therewith, the software

application including an associated engraved signature, the engraved signature being initially blank such that the software application can initially be used on one of a plurality of computer systems but once used on a computer system is authenticated for that particular computer system, the method comprising the steps of:

- during execution of the software application, reading the engraved signature;

- if the engraved signature is not blank, then performing the following:

- retrieving the identifier from the computer system;

- encrypting the identifier using an encryption method to obtain a computed signature;

- comparing the computed signature to the engraved signature; and

- inhibiting execution of the software application if the computed signature does not match the engraved signature; and

- if the engraved signature is blank, then performing the following:

- retrieving the identifier from the computer system;

- encrypting the identifier using the encryption method to obtain a computed signature; and

- storing the computed signature as the engraved signature thereby generating the engraved signature at the computer system on which the software application is being executed and authenticating the software application only for that computer system.

17. (New) A software protection system comprising:

- a computer system having an identifier;

- a software application loaded on said computer system and including an associated engraved signature, the engraved signature being initially blank such that the software application can initially be used on one of a plurality of

computer systems but once used on a computer system is authenticated for that particular computer system;

an authentication program executed by the computer system for authenticating the software application, during execution, the authentication program reading the engraved signature and;

if the engraved signature is not blank then performing the following:

retrieving the identifier from the computer system;

encrypting the identifier using an encryption method to obtain a computed signature;

comparing the computed signature to the engraved signature; and

inhibiting execution of the software application if the computed signature does not match the engraved signature; and if the engraved signature is blank then performing the following:

retrieving the identifier from the computer system;

encrypting the identifier using an encryption method to obtain a computed signature; and

storing the computed signature as the engraved signature thereby generating the engraved signature at the computer system on which the software application is being executed and authenticating the software application only for that computer system.